



## **Avaya Solution & Interoperability Test Lab**

---

# **Application Notes for configuring Avaya Aura® Communication Manager R6.2, Avaya Aura® Session Manager R6.2 and Avaya Aura® Application Enablement Services R6.2 to interoperate with ESTOS ECSTA – Issue 1.0**

### **Abstract**

These Application Notes describe the configuration steps required for ESTOS ECSTA to successfully interoperate with Avaya Aura® Communication Manager, Avaya Aura® Session Manager and Avaya Aura® Application Enablement Services. ESTOS ECSTA provides users with a TAPI to perform a variety of call handling scenarios.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

# 1. Introduction

These Application Notes describe the configuration steps required for ESTOS ECSTA to successfully interoperate with Avaya Aura® Communication Manager, Avaya Aura® Session Manager and Avaya Aura® Application Enablement Services (AES). ESTOS ECSTA is a Telephony Service Provider (TSP) for Microsoft TAPI 2.1, 2.2 and 3.0. This TAPI driver implements central communication between a PC and Avaya Aura® Communication Manager with Avaya Aura® Session Manager using CTI provided by AES. ESTOS Ephone is a test application which is used to verify successful communication between ESTOS ECSTA and AES and ensures call handling is completed as intended. ESTOS Ephone is a test tool provided by ESTOS for the purposes of demonstrating the abilities of ESTOS ECSTA only. The connection to AES is established by ESTOS ECSTA over the CSTA Phase III XML protocol using DMCC.

## 2. General Test Approach and Test Results

The interoperability compliance test included both feature functionality and serviceability testing. The feature functionality testing focused on a variety of inbound and outbound call handling scenarios to verify successful call control using the ECSTA TSP. The serviceability testing focused on verifying the ability of the ECSTA service to recover from disconnection and reconnection to the Avaya solution.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.ok

### 2.1. Interoperability Compliance Testing

Feature functionality testing included

- Conferencing.
- Consultative transfer.
- Blind transfer.
- Forwarding.
- DND (Do Not Disturb) with SAC (Send All Calls).
- Call waiting.
- Toggling between held calls.
- Activation/deactivation of the above features.
- Client authentication

These calls were placed and received using the Ephone test tool. Serviceability testing verified the ability of the solution to recover from simulated power and network failure.

### 2.2. Test Results

All tests were executed successfully with the following observations:

- If a call is placed from a SIP endpoint, e.g. extension 6002, during the period the G450 is disconnected, it fails to dial as expected. Upon reconnection of the G450, a call from the same extension also fails. A subsequent call from another extension to 6002 alerts the extension, however Ephone is unable to successfully answer the call. After a period of time this is resolved. The probable cause relates to AES timers.
- If Ephone is used to hangup a SIP initiated call e.g. Extn 6003 to 6002 during SIP Signalling interface outage, the SIP endpoint does not respond, both endpoints must end the call manually. This is expected. Once the SIP Signalling interface is returned to service, calls between 6003 and 6002 fail for a period, again the probable cause is due to AES timers.

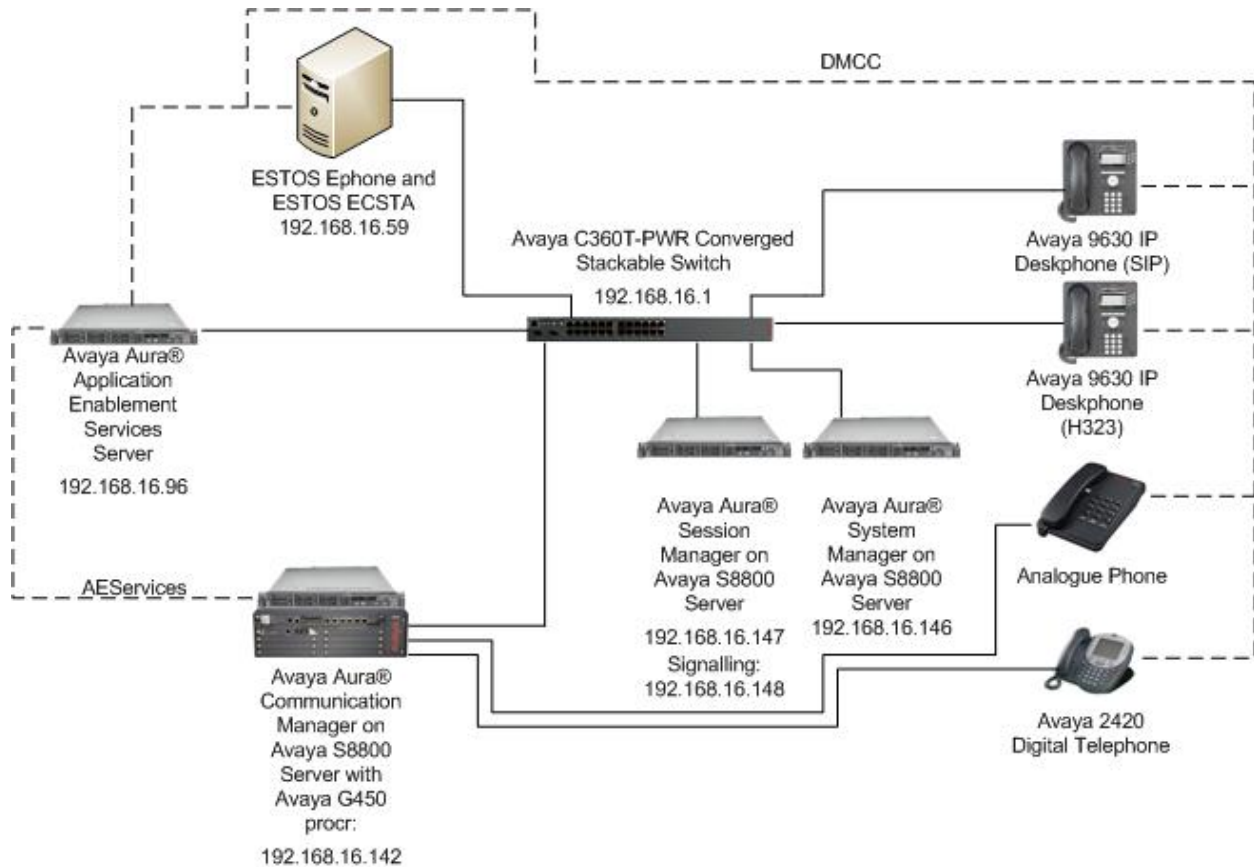
## 2.3. Support

Technical Support can be obtained for ESTOS products as follows:

- Online: <http://www.estos.com/contact/online-support-request.html>
- Phone: + 49 (8151) 36856-177

### 3. Reference Configuration

**Figure 1** illustrates the network topology used during compliance testing. The Avaya solution consists of an Avaya S8800 Server running Communication Manager with Avaya G450 Media Gateway as the PBX. An Avaya S8800 Server hosts the Application Enablement Services software. An Avaya S8800 Server pair host the System Manager and Session Manager components. Avaya 9600 series H323 and SIP IP telephones and 2400 series Digital telephones are connected to the PBX along with analogue endpoints and used in the testing. The ESTOS client is running on a Windows 2008 64bit server in a VMWare environment.



**Figure 1: Avaya Aura® Communication Manager and Avaya® Session Manager with Avaya Aura® Application Enablement Services Server and ESTOS Configuration**

## 4. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Equipment/Software	Release/Version
Avaya Aura® Communication Manager running on Avaya S8800 Server	R6.2 SP2
Avaya G450 Media Gateway <ul style="list-style-type: none"><li>• MM714</li><li>• MM712</li></ul>	31.22.0 HW3 FW73 HW7 FW9
Avaya Aura® Application Enablement Services running on Avaya S8800 Server	R6.2
Avaya Aura® System Manager running on Avaya S8800 Server	R6.2 SP2
Avaya Aura® Session Manager running on Avaya S8800 Server	R6.2 SP2
Avaya 9630 IP Telephone (H323)	3.104S
Avaya 9630 IP Telephone (SIP)	2.6.7.0
Avaya 2420 Digital Telephone	REL 6.00 HWT 51H FWV 6
Generic VMWare Server	Microsoft Windows 2008 Server R2 64bit ECSTA Avaya ACM 3.0.0.171 Ephone X64 3.20 (64 bit)

## 5. Configure Avaya Aura® Communication Manager

The configuration and verification operations illustrated in this section are performed using Communication Manager System Administration Terminal (SAT). The information provided in this section describes the configuration of Communication Manager for this solution. For all other provisioning information such as initial installation and configuration, please refer to the product documentation as referenced in **Section 11**. The configuration operations described in this section can be summarized as follows:

- Configure Coverage Path
- Configure Station Button Assignments
- Configure the Interface to AES
- Configure SIP endpoint for AES Control

## 5.1. Configure Coverage Path

In order to test DND, a cover path must be configured. Enter the command **add coverage-path next**, set **DND/SAC/Goto Cover** to **y**, configure **Point 1** as a station to which calls will be sent when DND is activated, in this case **1350**. Take a note of the **Coverage Path Number**.

```
add coverage path next                                     Page 1 of 1
                COVERAGE PATH
                Coverage Path Number: 1
                Cvg Enabled for VDN Route-To Party? n      Hunt after Coverage? n
                Next Path Number:                          Linkage
COVERAGE CRITERIA
  Station/Group Status   Inside Call   Outside Call
    Active?              n             n
    Busy?                y             y
    Don't Answer?       y             y      Number of Rings: 2
    All?                 n             n
  DND/SAC/Goto Cover?   y             y
  Holiday Coverage?     n             n
COVERAGE POINTS
  Terminate to Coverage Pts. with Bridged Appearances? n
  Point1: 1350          Rng:      Point2:
  Point3:                Point4:
  Point5:                Point6:
```

## 5.2. Configure Station Button Assignments

The application note assumes stations used are already configured on Communication Manager. Enter the command **change station x**, where **x** is the extension number to be controlled by the Ephone test tool. On **Page 1** configure **Coverage Path 1** with the coverage path created in **Section 5.1**, in this case **1**.

```
change station 4000                                     Page 1 of 5
                                                    STATION
Extension: 4000                                         Lock Messages? n          BCC: 0
Type: 2420                                             Security Code: 1234      TN: 1
Port: 01A0701                                         Coverage Path 1: 1      COR: 1
Name: Extn,4000                                       Coverage Path 2:        COS: 1
                                                    Hunt-to Station:
STATION OPTIONS
                                                    Time of Day Lock Table:
Loss Group: 2                                         Personalized Ringing Pattern: 1
Data Option: none                                     Message Lamp Ext: 4000
Speakerphone: 2-way                                   Mute Button Enabled? y
Display Language: english                             Expansion Module? n
Survivable COR: internal                               Media Complex Ext:
Survivable Trunk Dest? y                             IP SoftPhone? y
                                                    Remote Office Phone? n
                                                    IP Video Softphone? n
Short/Prefixed Registration Allowed: default
                                                    Customizable Labels? y
```

Navigate to **Page 4** and configure **send-calls** and **dn-dst** as button assignments, this will provide a visual indicator of when the Send All Calls and DND features are activated.

```
change station 4000                                     Page 4 of 5
                                                    STATION
SITE DATA
Room:                                                 Headset? n
Jack:                                                 Speaker? n
Cable:                                                Mounting: d
Floor:                                                Cord Length: 0
Building:                                             Set Color:
ABBREVIATED DIALING
List1:                                               List2:                   List3:
BUTTON ASSIGNMENTS
1: call-appr                                         5:
2: call-appr                                         6:
3: send-calls Ext:                                   7:
4: dn-dst                                           8:
voice-mail
```

### 5.3. Configure Interface to Avaya Aura® Application Enablement Services

Enter the node **Name** and **IP Address** for the Application Enablement Server, in this case **aesserver62** and **192.168.16.96** respectively. Take a note of the **procr** node **Name** and **IP Address** as it is used later in this section.

```
change node-names ip                                     Page 1 of 2
                                     IP NODE NAMES
Name                               IP Address
sm62sigint                         192.168.16.148
default                             0.0.0.0
aesserver62                       192.168.16.96
procr                             192.168.16.142
```

In order for Communication Manager to establish a connection to Application Enablement Services, administer the CTI Link as shown below. Specify an available **Extension** number, set the **Type** as **ADJ-IP**, which denotes that this is a link to an IP connected adjunct, and name the link for easy identification, in this instance, the node-name is used.

```
add cti-link 1                                         Page 1 of 3
                                     CTI LINK
CTI Link: 1
Extension: 5899
Type: ADJ-IP
                                     COR: 1
Name: aesserver62
```



Configure IP-Services for the AESVCS service using the **change ip-services** command. Using the procr node name as noted above i.e. **procr**

```
change ip-services Page 1 of 4
```

IP SERVICES					
Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port
AESVCS	y	procr	8765		

Navigate to **Page 4**, set the **AE Services Server** node-name and the **Password** the AES Server will use to authenticate with Communication Manager.

```
change ip-services Page 4 of 4
```

AE Services Administration				
Server ID	AE Services Server	Password	Enabled	Status
1:	aesserver62	Avayapassword1	y	in use

#### 5.4. Configure SIP Endpoint for AES Control

Each SIP endpoint to be controlled by ESTOS must be configured accordingly. Enter the command **change station xxxx** where xxxx is a SIP endpoint. Go to **Page 6** and in the **Type of 3PCC Enabled** enter **Avaya** as shown below.

```
change station 6002 Page 6 of 6
```

STATION	
SIP FEATURE OPTIONS	
Type of 3PCC Enabled: Avaya	
SIP Trunk: aar	

### 6. Configuration of Avaya Aura® Application Enablement Services

This section provides the procedures for configuring Application Enablement Services (AES). The procedures fall into the following areas:

- Create Switch Connection
- Create TSAPI Link
- Create CTI User
- Enable CTI User
- Configure DMCC Port
- Enable Security Database

## 6.1. Create Switch Connection

Access the OAM web-based interface of the Application Enablement Services Server, in this instance using the URL <https://192.168.16.96>, the Management console is displayed. Log in using the appropriate credentials.

The screenshot shows the Avaya Application Enablement Services Management Console login page. At the top left is the Avaya logo. The title is "Application Enablement Services Management Console". A red navigation bar at the top right contains a "Help" link. The main content area features a login form with the text "Please login here:" followed by "Username" and "Password" labels, each with an input field. Below the fields is a "Login" button. At the bottom of the page, there is a copyright notice: "© Copyright © 2009-2010 Avaya Inc. All Rights Reserved."

The **Welcome to OAM** screen is displayed next.

The screenshot shows the Avaya Application Enablement Services Management Console "Welcome to OAM" screen. At the top left is the Avaya logo. The title is "Application Enablement Services Management Console". On the right side, there is a welcome message and system information: "Welcome: User craft", "Last login: Sun Jul 29 18:01:18 2012 from 10.10.16.62", "Number of prior failed login attempts: 0", "HostName/IP: aesserver62/10.10.16.96", "Server Offer Type: TURNKEY", "SW Version: r6-2-0-18-0", and "Server Date and Time: Sun Jul 29 19:00:57 BST 2012". A red navigation bar at the top contains "Home" on the left and "Home | Help | Logout" on the right. On the left side, there is a vertical menu with the following items: "AE Services", "Communication Manager Interface", "Licensing", "Maintenance", "Networking", "Security", "Status", "User Management", "Utilities", and "Help". The main content area is titled "Welcome to OAM" and contains the following text: "The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:" followed by a bulleted list of domains and their descriptions. At the bottom of the main content area, there is a paragraph: "Depending on your business requirements, these administrative domains can be served by one administrator for all domains, or a separate administrator for each domain." At the bottom of the page, there is a copyright notice: "Copyright © 2009-2012 Avaya Inc. All Rights Reserved."

To establish the connection between Communication Manager and the Application Enablement Services Server, click **Communication Manager Interface** → **Switch Connections**. In the field next to **Add Connection**, enter **CM62** and click on **Add Connection**.

AVAYA **Application Enablement Services**  
Management Console

Welcome: User craft  
Last login: Wed Jun 20 19:50:09 2012 from  
Number of prior failed login attempts: 0  
HostName/IP: aesserver62/10.10.16.96  
Server Offer Type: TURKEY  
SW Version: r6-2-0-18-0  
Server Date and Time: Wed Jun 20 19:58:54 BST 2012

Communication Manager Interface | Switch Connections Home | Help | Logout

AE Services  
Communication Manager Interface  
Switch Connections  
Dial Plan  
Licensing  
Maintenance  
Networking  
Security  
Status  
User Management  
Utilities  
Help

Switch Connections

CM62 Add Connection

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<a href="#">Edit Connection</a> <a href="#">Edit PE/CLAN IPs</a> <a href="#">Edit H.323 Gatekeeper</a> <a href="#">Delete Connection</a> <a href="#">Survivability Hierarchy</a>			

The following screen will be displayed. Complete the configuration as shown and enter the password specified in **Section 5.3** when configuring AESVCS in ip-services. In this instance **Avayapassword1**, click **Apply** when done.

AVAYA **Application Enablement Services**  
Management Console

Communication Manager Interface | Switch Connections

AE Services  
Communication Manager Interface  
Switch Connections  
Dial Plan  
Licensing  
Maintenance  
Networking  
Security  
Status  
User Management  
Utilities  
Help

Connection Details - CM62

Switch Password

Confirm Switch Password

Msg Period  Minutes (1 - 72)

SSL

Processor Ethernet

[Apply](#) [Cancel](#)

The following screen will be displayed. Click on **Edit PE/CLAN IPs** in order to specify the IP address of the procr, as noted in **Section 5.3**



**Application Enablement Services**  
Management Console

Welcome: User craft  
Last login: Wed Jun 20 19:50:09 2012 from  
Number of prior failed login attempts: 0  
HostName/IP: sessserver62/10.10.16.96  
Server Offer Type: TURNKEY  
SW Version: r6-2-0-18-0  
Server Date and Time: Wed Jun 20 19:59:30 BST 2012

Communication Manager Interface | Switch Connections Home | Help | Logout

- ▶ AE Services
- ▼ Communication Manager Interface
  - Switch Connections
  - ▶ Dial Plan
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▶ Security
- ▶ Status
- ▶ User Management
- ▶ Utilities
- ▶ Help

### Switch Connections

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
CM62	Yes	30	0

Next to the **Add Name or IP** button, enter the IP address of the procr and click on **Add/Edit Name or IP**.



## Application Enablement Services Management Console

### Communication Manager Interface | Switch Connections

- ▶ AE Services
- ▼ Communication Manager Interface
  - Switch Connections
  - ▶ Dial Plan
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▶ Security
- ▶ Status
- ▶ User Management
- ▶ Utilities
- ▶ Help

#### Edit Processor Ethernet IP - CM62

The screen below will appear displaying the newly added Processor Ethernet IP



## Application Enablement Services Management Console

### Communication Manager Interface | Switch Connections

- ▶ AE Services
- ▼ Communication Manager Interface
  - Switch Connections
  - ▶ Dial Plan
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▶ Security
- ▶ Status
- ▶ User Management
- ▶ Utilities
- ▶ Help

Edit Processor Ethernet IP - CM62

Name or IP Address
<input type="text" value="16.142"/>

Select **AE Services** on the left pane and verify that the **DMCC Service** is licensed by ensuring that **DMCC Service** is in the list of services and that the **License Mode** is showing **NORMAL MODE**.

AE Services
Home | Help | Logout

- ▼ AE Services
  - ▶ CVLAN
  - ▶ DLG
  - ▶ DMCC
  - ▶ SMS
  - ▶ TSAPI
  - ▶ TWS
  - ▶ Communication Manager Interface
  - ▶ Licensing
  - ▶ Maintenance
  - ▶ Networking
  - ▶ Security
  - ▶ Status
  - ▶ User Management
  - ▶ Utilities
  - ▶ Help

### AE Services

---

IMPORTANT: AE Services must be restarted for administrative changes to fully take effect. Changes to the Security Database do not require a restart.

Service	Status	State	License Mode	Cause*
ASAI Link Manager	N/A	Running	N/A	N/A
CVLAN Service	OFFLINE	Running	N/A	N/A
DLG Service	OFFLINE	Running	N/A	N/A
DMCC Service	ONLINE	Running	NORMAL MODE	N/A
TSAPI Service	ONLINE	Running	NORMAL MODE	N/A
Transport Layer Service	N/A	Running	N/A	N/A

For status on actual services, please use [Status and Control](#)

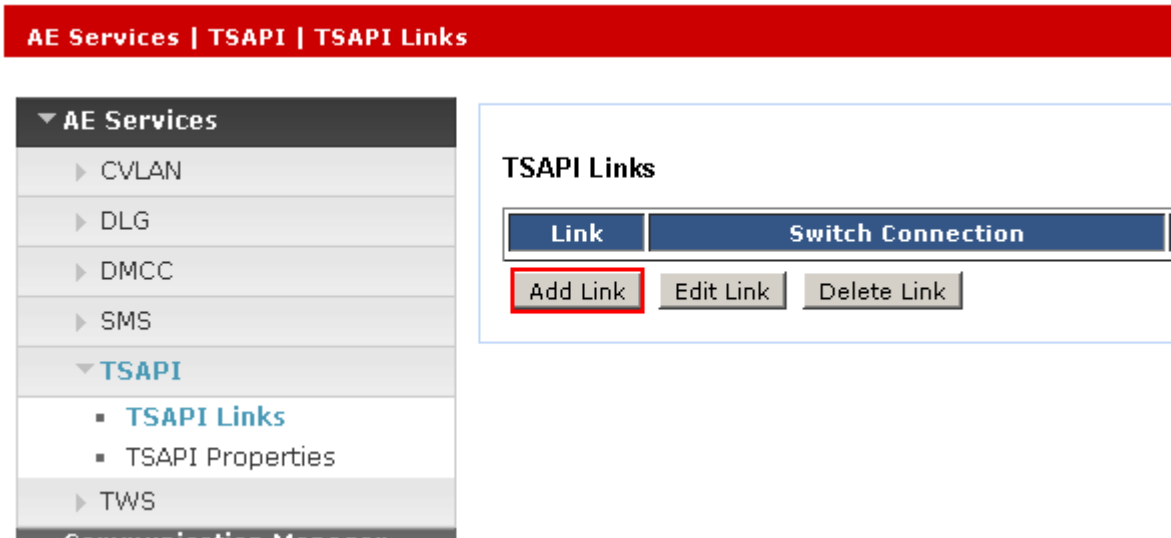
\* -- For more detail, please mouse over the Cause, you'll see the tooltip, or go to help page.

---

**License Information**  
 You are licensed to run Application Enablement (CT) release 6.x

## 6.2. Create TSAPI Link

A TSAPI link must be created, this will be configured for 3<sup>rd</sup> party applications to connect to AES. Click on **TSAPI** → **TSAPI Links** → **Add Link**.



AE Services | TSAPI | TSAPI Links

▼ AE Services

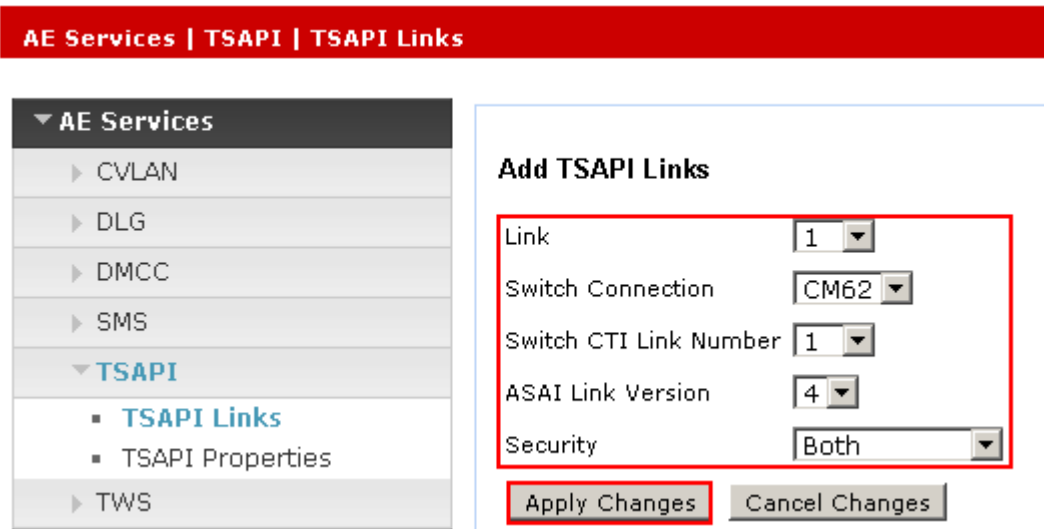
- ▶ CVLAN
- ▶ DLG
- ▶ DMCC
- ▶ SMS
- ▼ TSAPI
  - TSAPI Links
  - TSAPI Properties
- ▶ TWS

TSAPI Links

Link	Switch Connection
------	-------------------

Add Link Edit Link Delete Link

Select the **Link** number from the drop down box, select the administered **Switch Connection**, set the **Switch CTI Link Number** to **1**, the **ASAI Link Version** as **4** and set **Security** to **Both**, click **Apply Changes** when done.



AE Services | TSAPI | TSAPI Links

▼ AE Services

- ▶ CVLAN
- ▶ DLG
- ▶ DMCC
- ▶ SMS
- ▼ TSAPI
  - TSAPI Links
  - TSAPI Properties
- ▶ TWS

Add TSAPI Links

Link 1

Switch Connection CM62

Switch CTI Link Number 1

ASAI Link Version 4

Security Both

Apply Changes Cancel Changes



The following screen will appear advising to restart the TSAPI Server in order for the changes to take effect, click **Apply**

AE Services | TSAPI | TSAPI Links

- ▼ AE Services
  - ▶ CVLAN
  - ▶ DLG
  - ▶ DMCC
  - ▶ SMS
  - ▼ TSAPI
    - TSAPI Links
    - TSAPI Properties
  - ▶ TWS

### Apply Changes to Link

Warning! Are you sure you want to apply the changes?  
These changes can only take effect when the TSAPI server restarts.

**⚠ Please use the Maintenance -> Service Controller page to restart the TSAPI server.**

The following screen will appear displaying the newly added TSAPI Link, follow the changes in the screen above to restart the TSAPI server.

AE Services | TSAPI | TSAPI Links Home | Help | Logout

- ▼ AE Services
  - ▶ CVLAN
  - ▶ DLG
  - ▶ DMCC
  - ▶ SMS
  - ▼ TSAPI
    - TSAPI Links
    - TSAPI Properties
  - ▶ TWS

### TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
1	CM62	1	4	Both

### 6.3. Create CTI User

A user ID and password needs to be configured for ECSTA to communicate as a DMCC client with Application Enablement Services. Select **User Management** → **User Admin** → **Add User** from the left pane, to display the **Add User** screen in the right pane. Enter desired values for **User Id**, **Common Name**, **Surname**, **User Password** and **Confirm Password**. For **CT User**, select **Yes** from the drop-down list. Retain the default value in the remaining fields. Click **Apply** at the bottom of the screen (not shown below).

**User Management | User Admin | Add User**

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▶ Security
- ▶ Status
- ▼ **User Management**
  - ▶ Service Admin
  - ▼ **User Admin**
    - **Add User**
    - Change User Password
    - List All Users
    - Modify Default Users
    - Search Users
- ▶ Utilities
- ▶ Help

#### Add User

Fields marked with \* can not be empty.

* User Id	<input type="text" value="ctiuser"/>
* Common Name	<input type="text" value="ctiuser"/>
* Surname	<input type="text" value="ctiuser"/>
* User Password	<input type="password" value="....."/>
* Confirm Password	<input type="password" value="....."/>
Admin Note	<input type="text"/>
Avaya Role	<input type="text" value="None"/>
Business Category	<input type="text"/>
Car License	<input type="text"/>
CM Home	<input type="text"/>
Css Home	<input type="text"/>
CT User	<input type="text" value="Yes"/>
Department Number	<input type="text"/>

## 6.4. Enable CTI User

Navigate to the users screen by selecting **Security** → **Security Database** → **CTI Users** → **List All Users**. In the **CTI Users** window, select the user that was set up in **Section 6.3** and select the **Edit** option.

Security | Security Database | CTI Users | List All Users

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▼ Security
  - ▶ Account Management
  - ▶ Audit
  - ▶ Certificate Management
  - Enterprise Directory
  - ▶ Host AA
  - ▶ PAM
  - ▼ Security Database
    - Control
    - ▣ CTI Users
      - List All Users
      - Search Users

### CTI Users

User ID	Common Name
<input checked="" type="radio"/> ctuser	ctuser

The **Edit CTI User** screen appears. Tick the **Unrestricted Access** box and **Apply Changes** at the bottom of the screen.

Security | Security Database | CTI Users | List All Users

▶ AE Services	<b>Edit CTI User</b>	
▶ Communication Manager Interface	User Profile:	User ID: ctuser
▶ Licensing		Common Name: ctuser
▶ Maintenance		Worktop Name: NONE
▶ Networking		Unrestricted Access: <input checked="" type="checkbox"/>
▼ Security	Call and Device Control:	Call Origination/Termination and Device Status: None
▶ Account Management	Call and Device Monitoring:	Device Monitoring: None
▶ Audit		Calls On A Device Monitoring: None
▶ Certificate Management		Call Monitoring: <input type="checkbox"/>
Enterprise Directory	Routing Control:	Allow Routing on Listed Devices: None
▶ Host AA		
▶ PAM		
▼ Security Database		
▪ Control		

**Apply Changes** **Cancel Changes**

## 6.5. Configure DMCC Port

On the AES Management Console navigate to **Networking** → **Ports** to set the DMCC server port. During the compliance test, the **Unencrypted Port** set to **4721** was **Enabled** as shown in the screen below. Click the **Apply Changes** button (not shown) at the bottom of the screen to complete the process.

### Networking | Ports

▶ AE Services			
▶ Communication Manager Interface			
▶ Licensing			
▶ Maintenance			
▼ Networking			
AE Service IP (Local IP)			
Network Configure			
<b>Ports</b>			
TCP Settings			
▶ Security			
▶ Status			
▶ User Management			
▶ Utilities			
▶ Help			

Ports			Enabled	Disabled
CVLAN Ports				
Unencrypted TCP Port	9999		<input checked="" type="radio"/>	<input type="radio"/>
Encrypted TCP Port	<input type="text" value="9998"/>		<input checked="" type="radio"/>	<input type="radio"/>
DLG Port				
TCP Port	5678			
TSAPI Ports				
TSAPI Service Port	450		<input checked="" type="radio"/>	<input type="radio"/>
Local TLINK Ports				
TCP Port Min	1024			
TCP Port Max	1039			
Unencrypted TLINK Ports				
TCP Port Min	<input type="text" value="1050"/>			
TCP Port Max	<input type="text" value="1065"/>			
Encrypted TLINK Ports				
TCP Port Min	<input type="text" value="1066"/>			
TCP Port Max	<input type="text" value="1081"/>			
DMCC Server Ports				
Unencrypted Port	<input type="text" value="4721"/>		<input checked="" type="radio"/>	<input type="radio"/>
Encrypted Port	<input type="text" value="4722"/>		<input checked="" type="radio"/>	<input type="radio"/>
TR/87 Port	<input type="text" value="4723"/>		<input type="radio"/>	<input checked="" type="radio"/>

## 6.6. Enable Security Database

Select **Security** → **Security Database** → **Control** from the left pane, to display the **SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services** screen in the right pane. Uncheck **Enable SDB for DMCC Service** and click **Apply Changes**.

The screenshot shows a web interface with a left navigation pane and a main content area. The navigation pane is titled "Security" and includes the following items: AE Services, Communication Manager Interface, Licensing, Maintenance, Networking, Security (expanded), Account Management, Audit, Certificate Management, Enterprise Directory, Host AA, PAM, Security Database (expanded), Control (selected), and CTI Users. The main content area is titled "SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services" and contains two checkboxes: "Enable SDB for DMCC Service" (unchecked) and "Enable SDB for TSAPI Service, JTAPI and Telephony Web Services" (unchecked). Below the checkboxes is an "Apply Changes" button. Red boxes highlight the checkboxes and the button in the original image.

**Security | Security Database | Control**

**SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services**

- Enable SDB for DMCC Service
- Enable SDB for TSAPI Service, JTAPI and Telephony Web Services

**Apply Changes**

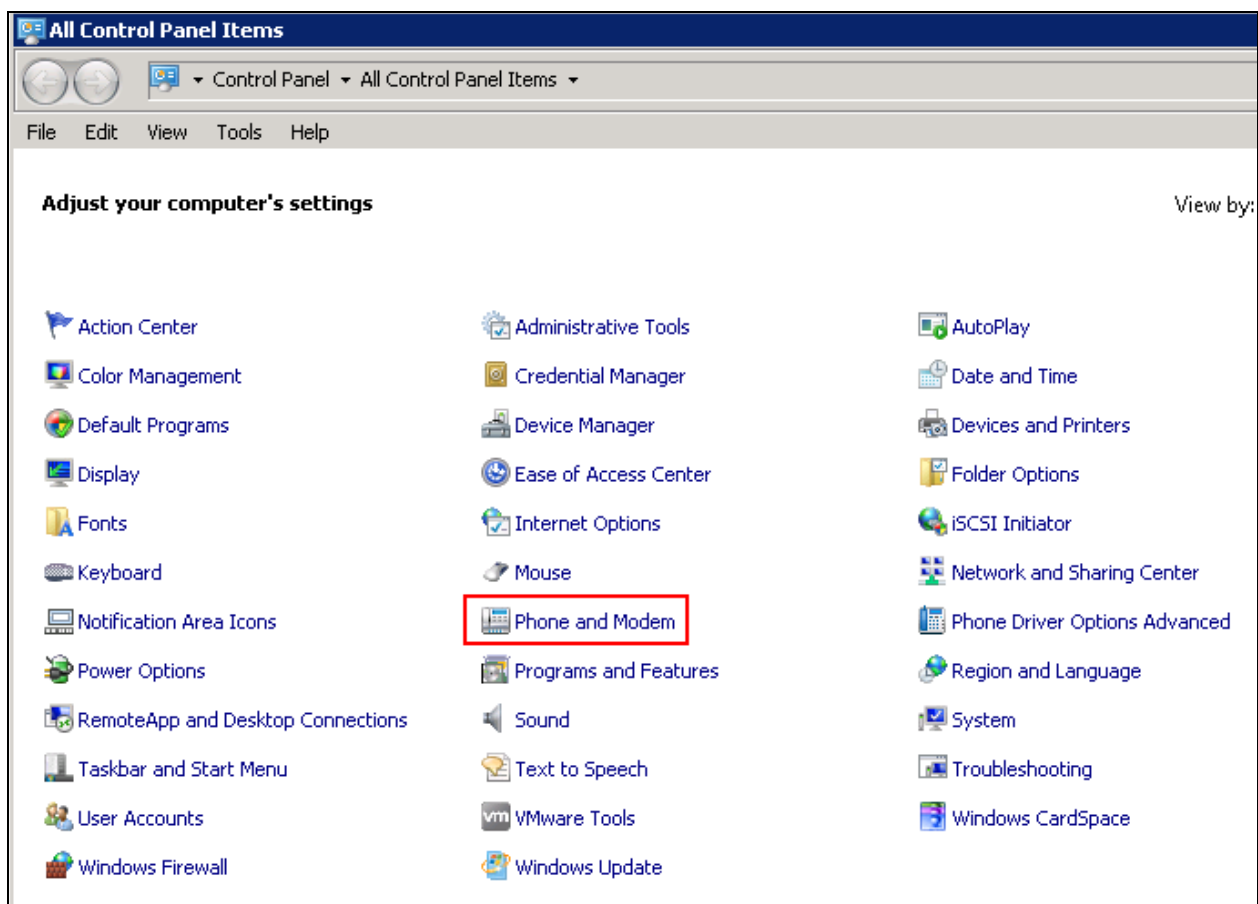
## 7. Configure ESTOS ECSTA

ESTOS ECSTA is installed using a Microsoft Installer package. These Application Notes assume installation of ECSTA has been completed, the subsequent configuration of ECSTA can be summarized as follows:

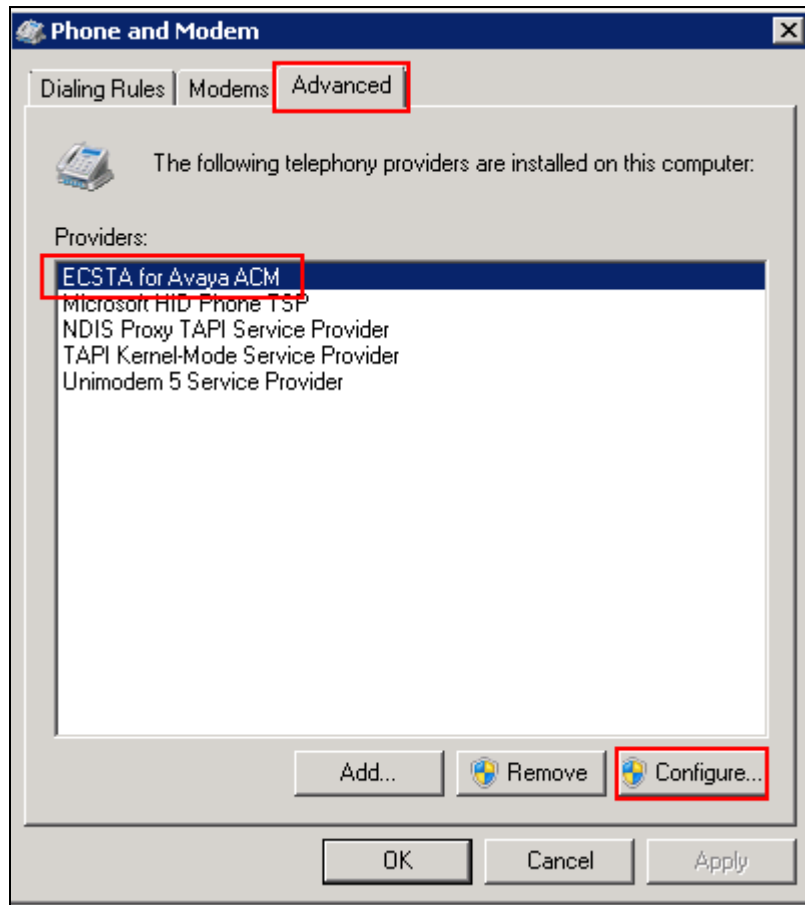
- Configure CTI Parameters
- Configure Extensions to be Controlled

### 7.1. Configure CTI Parameters

In order to establish connectivity to the AES, ECSTA must be configured with the appropriate settings. On the PC hosting the ECSTA client, access the Windows Control Panel and double click on **Phone and Modem**.



Click the **Advanced** tab, select **ECSTA for Avaya ACM** and click **Configure**.





The ECSTA configuration screen will appear, in the **AES Connection** section configure the **Hostname or IP – Port** with the AES IP Address and the DMCC port configured in **Section 6.5**. Click the radio button next to **TCP Connection (not encrypted)**. In the **Login** section specify the **CTI User** and **Password** configured in **Section 6.3**, in the **Communication Manager Name** field enter the name of the switch connection created in **Section 6.1**.

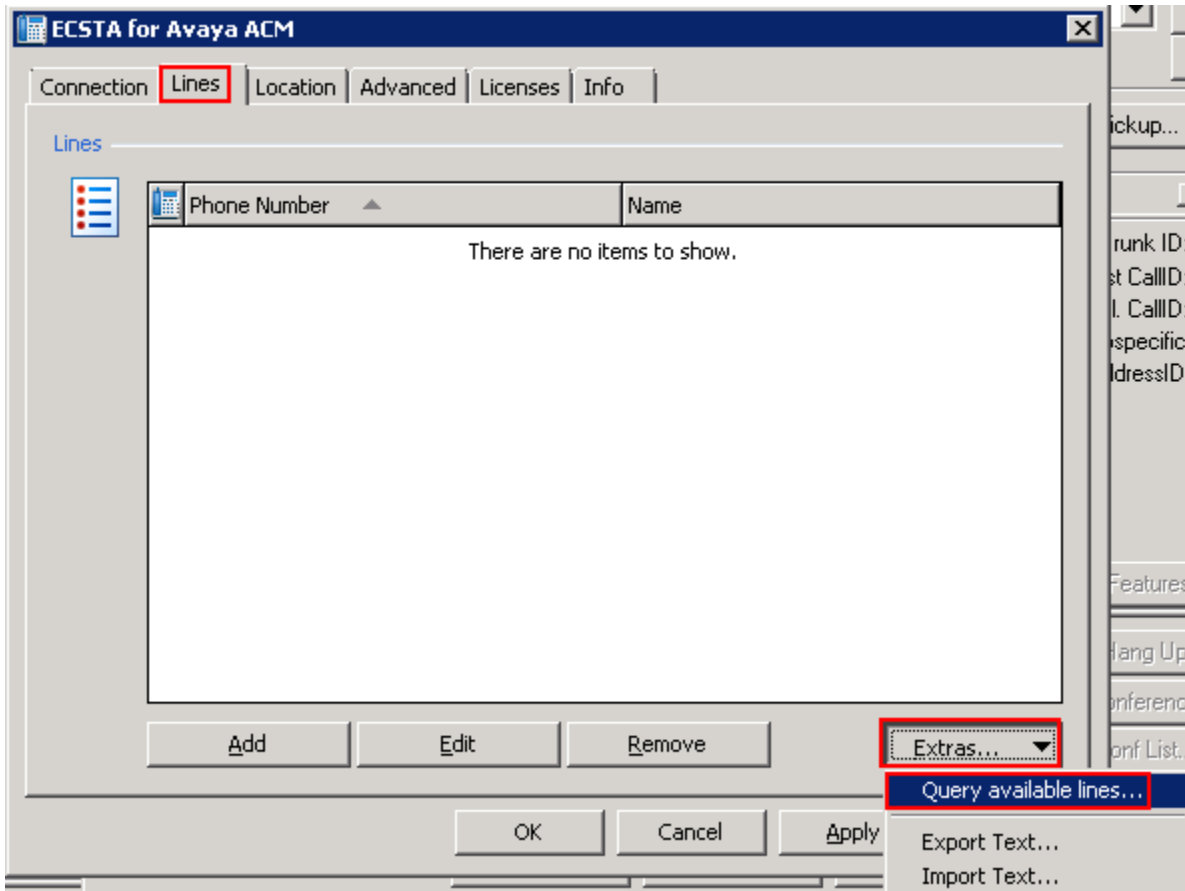
The screenshot shows the 'ECSTA for Avaya ACM' configuration window. The 'Connection' tab is active, and the 'AES Connection' section is expanded. The 'Host Name or IP - Port' field is set to '16.96' and '4721'. The 'TCP Connection (not encrypted)' radio button is selected. The 'Login' section shows the 'User' field set to 'ctiuser', the 'Password' field set to '\*\*\*\*\*', and the 'Communication Manager Name' field set to 'CM62'. The 'Comments for this connection' field is empty. The 'OK', 'Cancel', 'Apply', and 'Help' buttons are visible at the bottom.

Field	Value
Host Name or IP - Port	16.96
Port	4721
Connection Type	TCP Connection (not encrypted)
User	ctiuser
Password	*****
Communication Manager Name	CM62

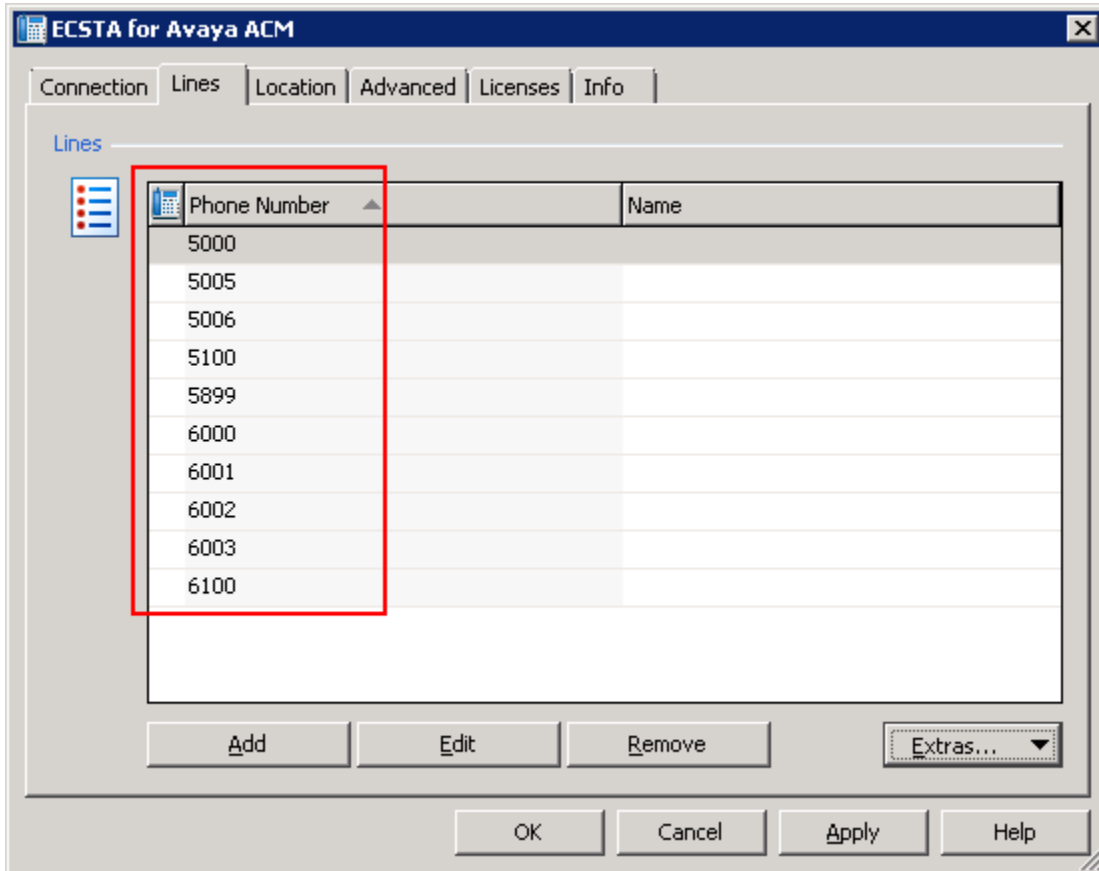
Click on the **Locations** tab, in the **First Extension (Phone Number)** and **Last Extension (Phone Number)** fields enter the first and last extension numbers for the range of extensions to be controlled.

The screenshot shows the 'ECSTA for Avaya ACM' application window with the 'Location' tab selected. The 'Location' section includes a globe icon, a 'Use Location' checkbox, and three input fields: 'Country Code' (value: 1 for USA), 'Area Code' (value: 212 NY City), and 'Local Office Code' (value: 1234 for Company). The 'Phone Number Range' section contains two input fields: 'First Extension (Phone Number)' (value: 5000, e.g. 10) and 'Last Extension (Phone Number)' (value: 6100, e.g. 350). The 'Phone Number Format' section has a text box with the instruction 'You may apply rules for formatting of phone numbers.' and an 'Edit Format...' button. At the bottom are 'OK', 'Cancel', 'Apply', and 'Help' buttons.

Click the **Lines** tab and click **Extras**, from the menu which appears, click **Query Available Lines**. This will interrogate Communication Manager for all extensions available in the range defined in the Location tab.



The following screen will be displayed showing the extensions available from Communication Manager. Click on **OK** when done.

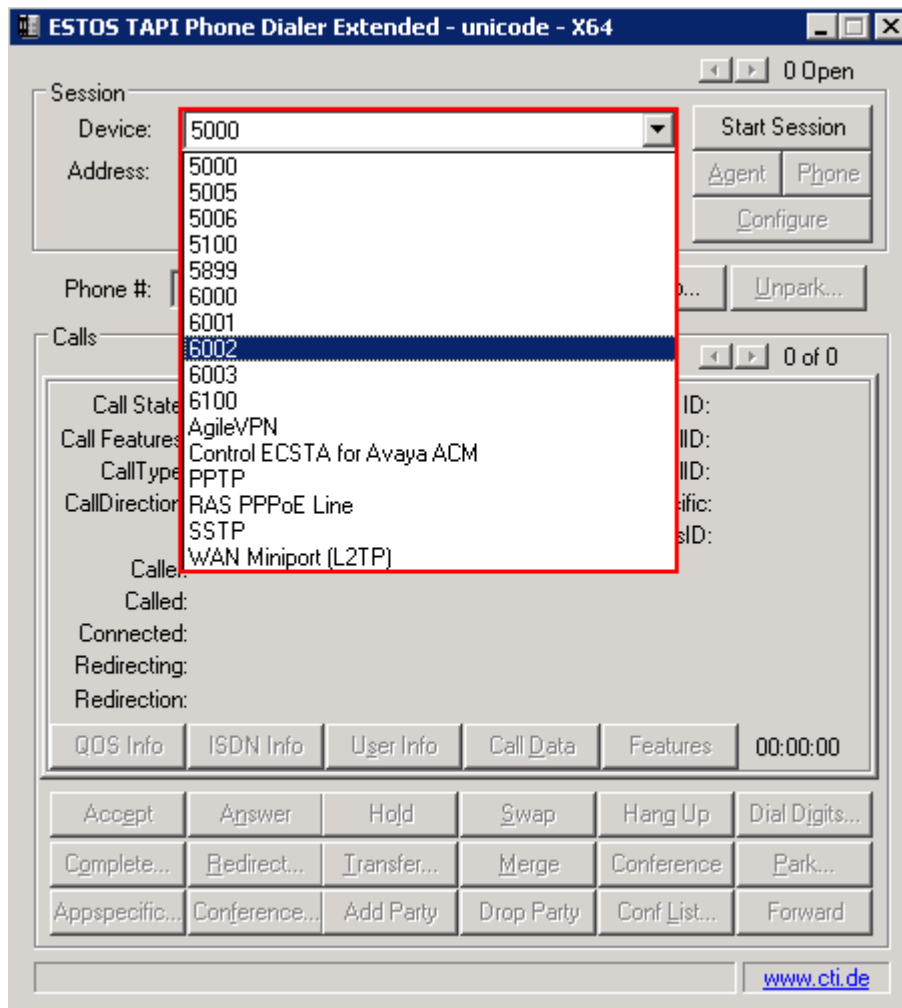


## 8. Configure ESTOS Ephone Test Tool

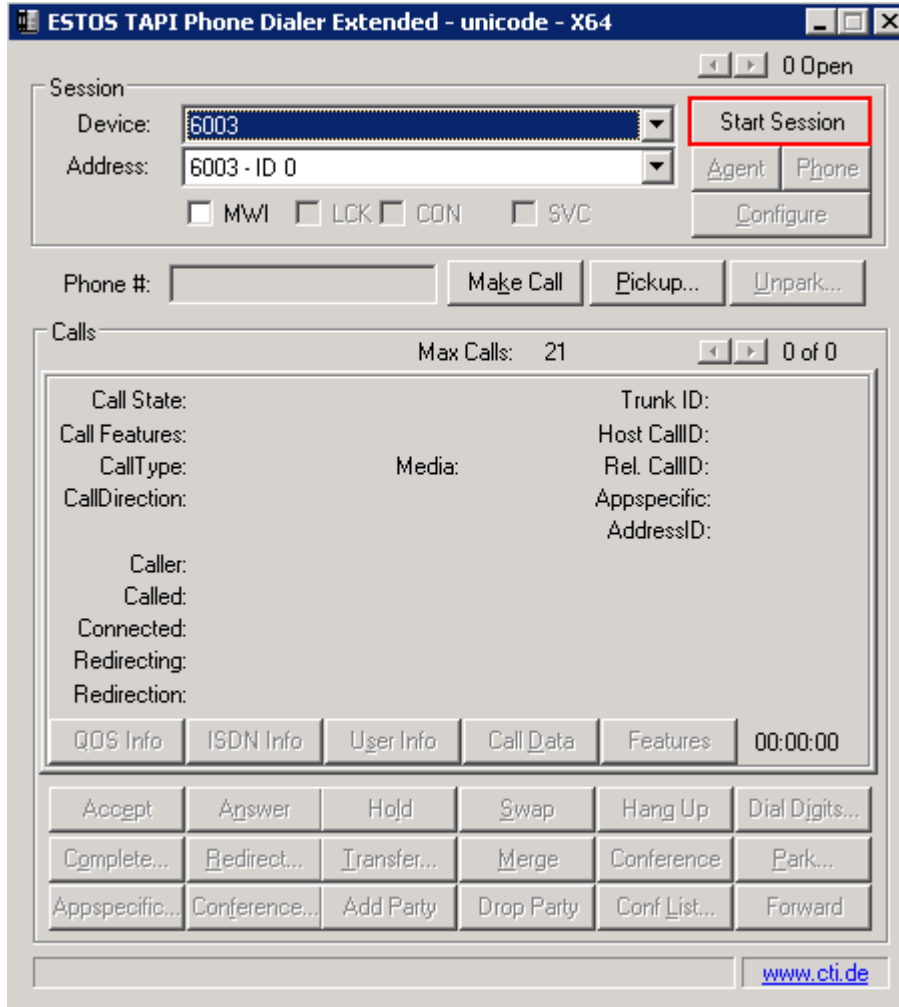
ESTOS Ephone is a test tool provided by ESTOS for the purposes of demonstrating the abilities of ESTOS ECSTA only, and is not a product available for purchase. The Ephone test tool used to verify connectivity and call control to Communication Manager using CTI provided by AES through the ECSTA connection. Double click on the EPhoneX64 icon on the desktop.



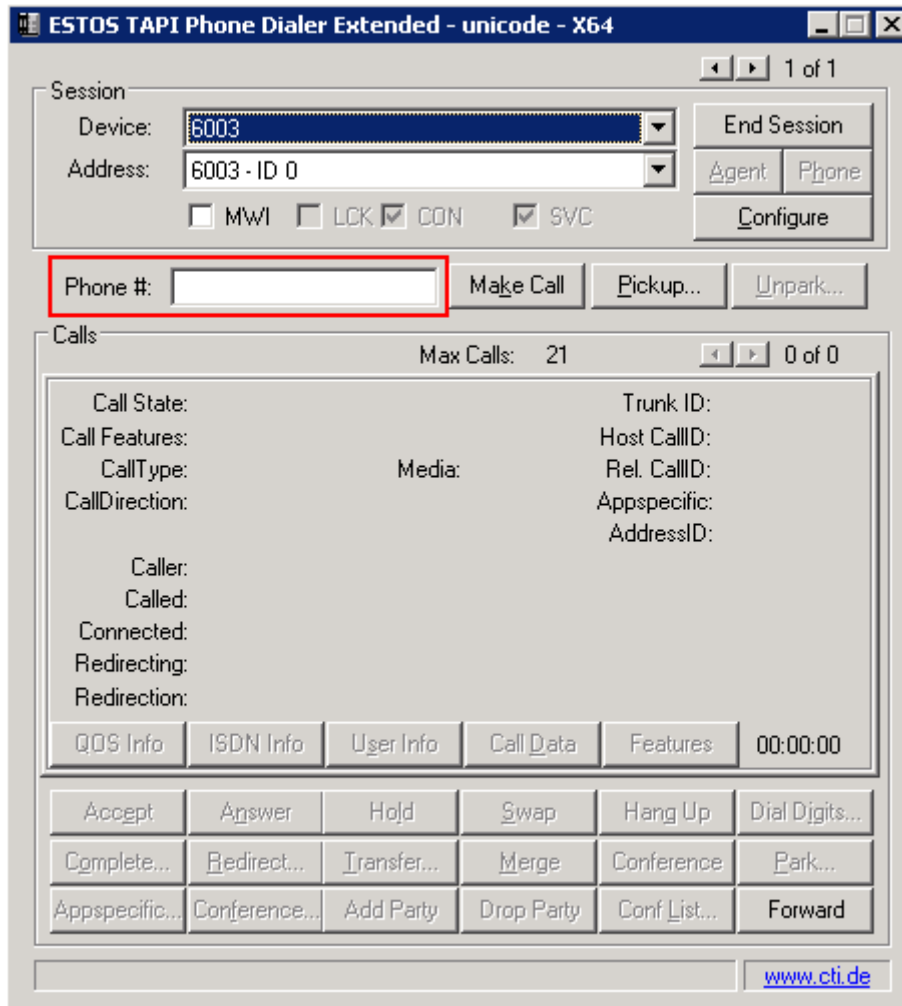
The application will load. Select the extension to be controlled from the drop down list.



Click on **Start Session** in order to begin control of the selected extension.



The screen shown below will be displayed. Note that it is now possible to enter a number in the **Phone #** field.



## 9. Verification Steps

This section provides tests that can be performed to verify correct configuration of the Avaya and ESTOS solution.

### 9.1. Verify Avaya Aura® Communication Manager CTI Service State

The following steps can ensure that the communication between Communication Manager and the Application Enablement Services server is functioning correctly. Check the AESVCS link status with Application Enablement Services by using the command **status aesvcs cti-link**. The CTI link is 1. Verify the **Service State** of the CTI link is **established**.

```
status aesvcs cti-link
```

AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	<b>Service State</b>	Msgs Sent	Msgs Rcvd
1	4	no	aesserver62	<b>established</b>	18	18



## 9.2. Verify Avaya Aura® Application Enablement Services DMCC Service

The following steps are carried out on the Application Enablement Services to ensure that the communication link between ECSTA and the Application Enablement Services server is functioning correctly. Verify the status of the DMCC service by selecting **Status → Status and Control → DMCC Service Summary**. The **DMCC Service Summary – Session Summary** screen is displayed as shown below. It shows a connection to the ESTOS client, IP address **192.168.16.59**. The **Application** is shown as **ECSTA for AvayaACM** and the **Far-end Identifier** is given as the IP address **192.168.16.59** as expected, the **User** is displayed as the user configured for use by ECSTA.

Status | Status and Control | DMCC Service Summary Home | Help | Logout

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▶ Security
- ▼ **Status**
  - Alarm Viewer
  - ▶ Logs
  - ▼ **Status and Control**
    - CVLAN Service Summary
    - DLG Services Summary
    - **DMCC Service Summary**

### DMCC Service Summary - Session Summary

Enable page refresh every  seconds

Session Summary [Device Summary](#)  
Generated on Sun Jul 29 19:45:39 BST 2012

Service Uptime: 4 days, 11 hours 6 minutes

Number of Active Sessions: 1

Number of Sessions Created Since Service Boot: 4

Number of Existing Devices: 0

Number of Devices Created Since Service Boot: 0

	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	62A9AD6B9A9CA14E7 9BCFB7524DFCF20-3	ctiuser	ECSTA for Avaya ACM	192.168.16.59	XML Unencrypted	0

## 9.3. Verify Connection of ESTOS ECSTA to Avaya Aura® Application Enablement Services

Navigate to the ESTOS log files contained in **c:\ecstaACM** and open **general5\_0.txt**. Verify connectivity with the AES (**10.10.16.30**) on port **4721** by the Ephone test tool controlling extension **4000** via ECSTA, as shown in the log extract below. **LineOpen** confirms successful connection.

```

25.07.2012 09:03:53:387;32;5000;TSPI_lineOpen begin
25.07.2012 09:03:53:387;32;5000;TSPI_lineOpen success
25.07.2012 09:03:53:387;32;TSPI_lineSetDefaultMediaDetection;5000 MediaModes 00000004
25.07.2012 09:03:53:387;32;ETspBase::ConnectionWatchFunction;PBX Connect is required
25.07.2012 09:03:53:387;32;ETspBase::Connect;ETspBase::Connect TCP: Host
192.168.16.96, Port 4721
25.07.2012 09:03:53:653;32;ETspBase::ConnectionWatchFunction;Connect result: 00000000
25.07.2012 09:03:53:778;32;5000;LineOpen 00000000
    
```

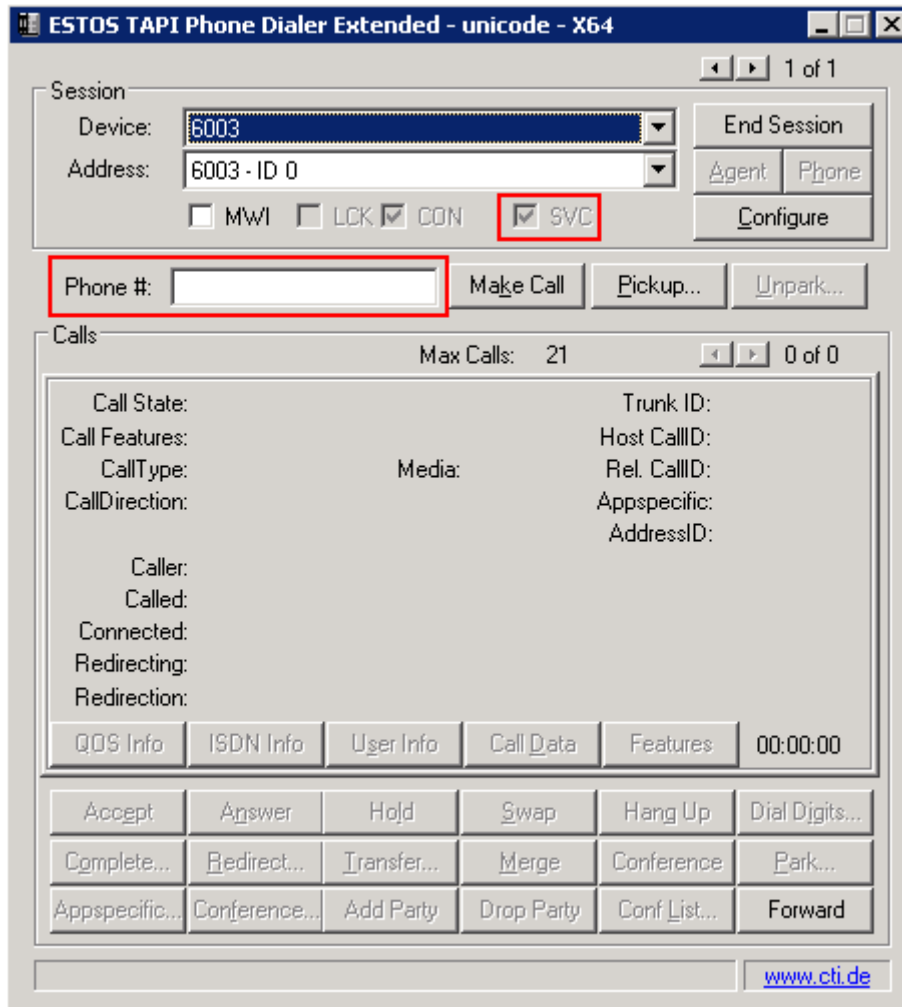
RCP; Reviewed:  
SPOC 9/23/2012

Solution & Interoperability Test Lab Application Notes  
©2012 Avaya Inc. All Rights Reserved.

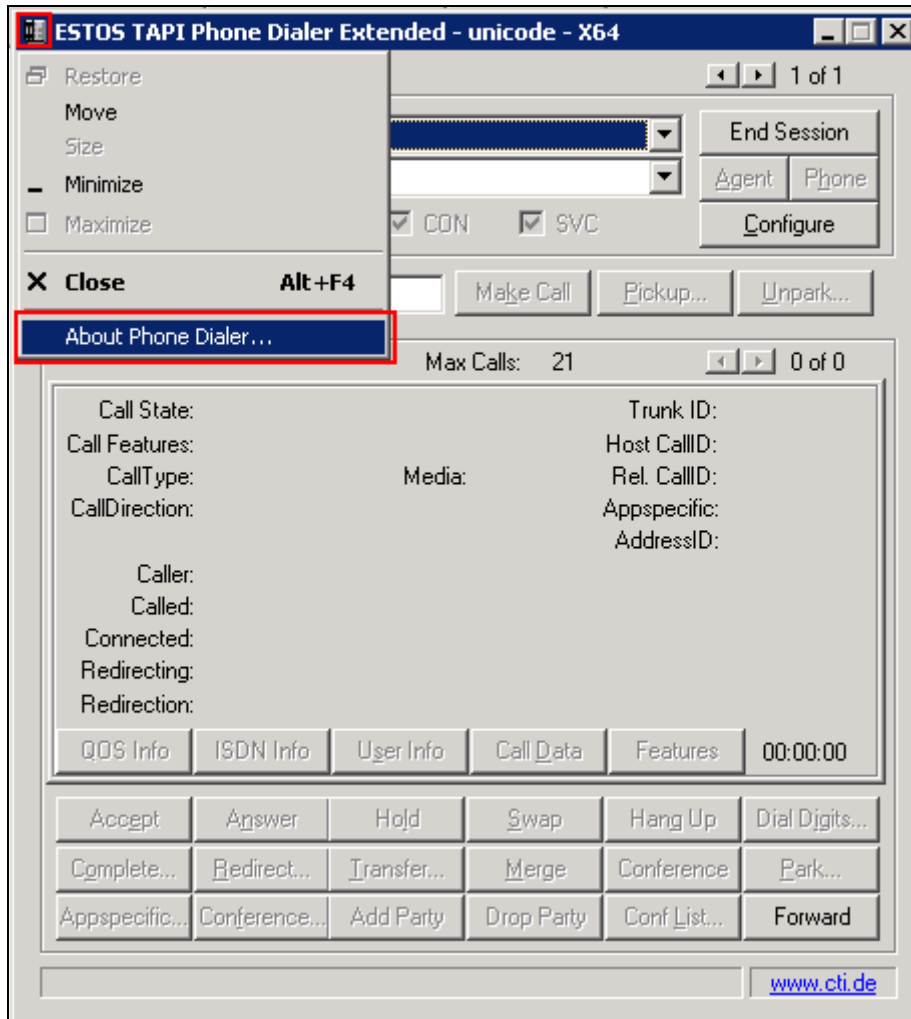
33 of 37  
ESTOSCMAESSM62

## 9.4. Verify Connectivity of ESTOS Ephone test tool to the Avaya Solution

Select the extension to be controlled from the drop down list and click **Start Session**. Verify that the EPhone test tool is connected with the presence of a tick in the **SVC** box and the availability of the **Phone #** field, highlighted in the screen shot below



Click on the top left corner of the Ephone test tool and select **About Phone Dialer** from the menu that appears.



Verify the version is as expected.



## 10. Conclusion

These Application Notes describe the configuration steps required for ESTOS ECSTA to successfully interoperate with Avaya Aura® Communication Manager, Avaya Aura® Session Manager and Avaya Aura® Application Enablement Services. All functionality and serviceability test cases were completed successfully with observations noted in **Section 2.2**.

## 11. Additional References

Product documentation for Avaya products may be found at <http://support.avaya.com>

[1] Avaya Aura® Application Enablement Services Administration and Maintenance Guide–  
Release 6.2, Issue 1, July 2012

[2] Administering Avaya Aura® Communication Manager – Release 6.2, Issue 7.0, July 2012

Product documentation for ESTOS products can be found at <http://www.estos.de>

---

**©2012 Avaya Inc. All Rights Reserved.**

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at [devconnect@avaya.com](mailto:devconnect@avaya.com).